REMARKS

This Supplemental Amendment is submitted to properly identify the status of Currently Amended Claim 1.

Claims 1-2, 4-12, 14-22, and 29-31 were rejected under 35 USC 103 as being unpatentable over Williams US Patent 6,304,973 in view of Ichikawa et al, US Patent 6.307,837. Applicant respectfully traverses.

With respect to claims 1, 11, and 21, the Examiner states the Williams teach a method for filtering packets using a policy. That, basically, merely states that the intended goal is roughly the same, but that is not saying much, since it is the steps taken to reach the goal, i.e., the method steps themselves, that matter.

Williams teaches the notion of identifying and verifying a user of a terminal, that that is not related to filtering of packets. Correctly, the Examiner does not focus on this aspect of the Williams reference but, rather, focuses on the notion of employing a policy in connection with filtering a packets -- which is the goal of applicant's claimed method. Indeed, the passage cited by the Examiner in support of his assertion of what Williams teaches (col. 15, line 66 - col. 16, line 25) teaches that there is "rudimentary port filtering based on TCP and UDP ports." However, the TCP and UDP ports are *process* identifiers -- not hardware/compute/hosts identifiers (see col. 16, lines 5-8), and the policy related to this filtering specifies which source *processes* can communicate with which *destination* processes.

The Examiner continues by admitting that "Williams fails to specifically teach verifying the first device (source address) that is included in the transferred packet" but that "Ichikawa et al teaches a method for packet transferring at the start of communication using a gateway to authenticate the identity of the remote terminal...." It is true that Williams does not authenticate the source address of packets in connection with which the policy regarding communication between processes is enforced, and it is true that Ichikawa et al teach authenticating identity of remote terminals. However, Ichikawa et al authenticate remote terminals in a process that is different from the process defined in claim 1. Specifically, with reference to the Ichikawa et al FIG. 3 and the associated text at col. 7 line 45 to col. 8, line 18, the Ichikawa et al initial authentication steps are as follows.

- When starting communication, a wireless packet terminal 1-7 sends a communication startup request signal (2-1) to the wireless base station 1-6.
- The wireless base station 1-6 receives the communication startup request signal in the terminal authentication section 10, and sends a terminal information request (2-2) to the terminal authentication server 1-8.
- In response, terminal authentication server 1-8 forwards terminal information notice to the wireless base station 1-6.
- Upon receiving the terminal information notice (2-3), terminal authentication section 10 stores the received terminal information in the terminal information memory section 11.
- Next, terminal authentication section 10 generates a random number for the purpose of terminal authentication and prepares an encryption of the random number using the encryption key provided in the terminal information, and the encrypted random number is sent, as the authentication request signal (2-4) to wireless packet terminal 1-7.
- Wireless packet terminal 1-7 decodes the encrypted random number received from the wireless base station 1-6 using the encryption key which had been pre-notified by the wireless packet network, and sends the result back to the wireless base station 1-6 as the authentication response signal (2-5).
- Wireless base station 1-6 compares returned random number with the random number, previously sent as the authentication request signal from the terminal authentication section 10.
- When the two random numbers match, terminal authentication section 10 decides that wireless packet terminal 1-7 is an authorized terminal, and so notifies the wireless packet terminal 1-7, using the authentication reception signal (2-6), that the communication is allowed.

- From this point on, the packet encrypting section 12 encrypts only the data section of the data packet (except the header section), using the encryption key received from terminal authentication section 10, and transmits the encrypted data.

To summarize the above, the wireless station enlists the assistance of the terminal authentication system, and can be viewed as a group. So viewed, the process is as follows: the terminal identifies itself, the group chooses a random number, encrypts it, and sends it to the terminal, as a challenge. The terminal decrypts the challenge, and returns the random number. Thereafter, packets are sent where the data portion is encrypted, and the header portion is not.

Incorporating the teachings of Ichikawa et al into the Williams arrangement, the packets where a policy is enforced relative to the TCP and UDP addresses would have the data portion encrypted, and the header portion not encrypted, following an initial identification and authentication process where the terminal seeking connection would have to correctly respond to a challenge.

In contradistinction to the teachings of Ichikawa et al, claim 1 specifies that (1) the received packet contains an encrypted identifier, and an unencrypted remainder, (2) the encrypted identifier is authenticated (which necessarily means decrypting the identifier), and (3) forwarding the packet, if appropriate.

As for the initial communication according to the Ichikawa et al teachings, the response to the challenge is not an encrypted identifier. It is not something that needs to be decrypted in order to authenticate the terminal. Moreover, it is not forwarded to a second device. As for subsequent packets, their structure is precisely the opposite of the structure specified in claim 1. That is, whereas claim 1 specifies packets where the data is in the clear, and the identifier is encrypted, the Ichikawa et al reference teaches encrypting the data, and the header in the clear.

Therefore, it is respectfully submitted that claim 1 is not obvious in view of the Williams and Ichikawa et al references.

The above analysis pertains to question of the authentication teachings of Ichikawa as they relate to claim 1. It should be noted that it is independent of **what** is being authenticated.

The above arguments apply with equal force to claim 11, and therefore applicant believed that claim 11 is not obvious in view of the Williams and Ichikawa et al references.

As for claim 21, it specifies receiving a packet that includes an "encrypted common host identifier." As for the initial Ichikawa et al communication, neither the encrypted random number of the challenge nor the returning random number of the response constitute an "encrypted common host identifier." As for the subsequent communication, it is expressly taught that the data is encrypted and the header is not. Therefore, the teachings of Ichikawa et al, if anything, teach away from the subject matter of claim 21 (as is the case with respect to claims 1 and 11).

The above analysis pertains to the question of the authentication teachings of Ichikawa as they relate to claims 1, 11, and 21, independently of **what** is being authenticated. It should be noted, however, there is no motivation for authenticating TCP or UDP ports. The Williams reference concerns itself with authenticating users, not the sources (hosts/terminals) from where the users operate, and concerns itself with processes that are, or are not, allowed to conduct communication (based on a policy). Authentication of the user appears to satisfy Williams. Since there is no knowledge of any spoofing of process ports, there is no motivation for authenticating process ports.

In connection with claims 1, 11, and 21, the Examiner asserted that the teachings of Williams' teachings of applying a policy whereby a packet is allowed, or disallowed based on TCP and UDP ports and a policy pertaining to ports might be modified by the teachings of Ichikawa regarding authentication, it is assumed that the rejection of the dependent claims is also based on this assertion. It is respectfully submitted that, based on the above remarks, all of the dependent claims are not obvious in view of the cited combination of references. Additionally, at least some of the dependent claims contain limitations that make the claims even more not obvious.

For example, with respect to claims 5, 15, and 30, the Examiner asserts that "Williams as modified teaches retrieving security from authentication header, retrieving a key with security, and determining if packet is authentic using a key." In support of this assertion, the Examiner cites Ichikawa et al, col. 11, lines 59 to col. 12, line 60. The teachings in the cited passage, however, address the encryption key that is stored in association with each recognized terminal, and though the Examiner might somehow interpret the teachings by Ichikawa et al regarding the retrieving of the encryption key as "retrieving a pointer to a security association" it is clear that such retrieving is not "from an authentication header from said packet." The encryption key is not retrieved from a header, and nor is the information that is used to retrieve the encryption key (if the Examiner were to argue that the information

Of course, citing the Ichikawa et al reference when making an assertion comparing authenticated identifier by the step of authenticating to a list of identifiers, retrieving at least one policy result relative to the authenticated identifier, [and] determining whether to send the packet to the second device in accordance to the policy rule." Respectfully, applicant disagrees.

It is admitted that Williams teaches a policy based, which can be viewed as identifiers. Therefore, it is assumed that the Examiner's reference to Williams "as modified" and the citation to cols. 8 and 0 of Ichikawa et at relates to the assertion that the "authenticating to a list of identifiers." Applicant respectfully submits that, assuming that to be valid, nevertheless claims 2 and 12 are patentable because there is no step of denidng to a third device., on TCP and UDP ports First, as indicated above, there is absolutely no motivation for authenticating TCP and UDP ports. Therefore, modification of Williams according to the teachings of Ichikawa et al would not tackle the issue of authenticating TCP and UDP ports. If at all, the teachings of Ichikawa et al might be applied to the issue of authenticating users.

Second,

Dated: 1/6/05

Respectfully,
Steven M. Bellovin

By
Henry T. Brendzel
Reg. No. 26,844
Phone (973) 467-2025
Fax (973) 467-6589
email brendzel@comcast.net